REMARKS

Claims 1-27 are pending in this application. By this Amendment, the drawings are replaced pursuant to the attached drawing sheets, and the specification and claims 1, 18 and 20-27 are amended. Fig. 1 corrects labels "12" and "17" by their interchange, and all of Figs. 1-24 incorporate the corrections indicated in the original drawings. Claims 1, 18 and 20-27 are amended to recite features supported in the specification at, for example, page 31, lines 15-18; page 33, lines 2-20; page 37, lines 7-23, and Figs. 9-11. No new matter is added by any of these amendments.

Applicants appreciate the courtesies extended to Applicants' representative, Mr. Choi, by Examiner Colin during the December 14, 2004 interview. The points discussed during the interview, in so far as applicable to the new grounds for rejection, are incorporated in the remarks below and constitute Applicants' record of the interview.

In particular, Applicants' representative argued that the claimed features, as presented in the September 29, 2004 Amendment, obviate the rejection under 35 U.S.C. §103(a) over U.S. Patent 6,189,146 to Misra *et al.* issued in the March 29, 2004 Final Office Action. Examiner Colin agreed to review the arguments further before issuing another action, which was done.

The newly issued Office Action rejects claims 1-27 under 35 U.S.C. §103(a) over U.S. Patent 5,117,096 to Bauer *et al.* (hereinafter "Bauer") in view of U.S. Patent Publication 2002/0013898 to Sudia *et al.* (hereinafter "Sudia"). This rejection is respectfully traversed.

Bauer and Sudia, alone or in combination, do not teach or suggest a distribution information management system having at least a structure comprising a data carrier attached to an article, a distribution information processing module, and a distribution information management module the distribution information processing module including at least an information generating unit that processes the information to be stored in the data carrier, wherein the information includes at least a signer identifier that is a receiver identifier of last information stored in the data carrier, the information generating unit comprising at least a signature module that performs signature generating process, the signature module comprising a signature part that generates the digital signature for the information generated by the distribution information generating part; a first signer private information storage part that stores signer private information used by the signature part for generating the digital signature; and a signature key use limit information storage part that stores a signer key use limit information to indicate whether the signature key information is already used, as recited in claim 1, and similarly recited in claims 20, 26 and 27.

Moreover, Bauer and Sudia both fail to teach or suggest a data carrier attached to an article for storing information including at least a signature key use limit information storage part that stores a signer key use limit information to indicate whether the signature key information is already used, as recited in claim 18.

Further, Bauer and Sudia, alone or in combination, do not to teach or suggest a distribution information management module that includes at least a signature key information generating unit that processes the signature key information to be sent to the distribution information processing module responsive to a signer key use limit information indicating that the signature key information is not already used, as recited in claim 21.

Neither Bauer nor Sudia, alone or in combination, teaches or suggests a distribution information processing method including at least a signature sub-step that includes at least a signature key use limit information checking micro-step for checking signer key use limit information to indicate whether the signature key information is already used, as recited in claim 22, and similarly recited for a computer program in claim 24.

In addition, Bauer and Sudia do not teach or suggest a distribution information management method including at least a signature key information generating sub-step for generating a signature key information used by the distribution information processing module for generating a distribution information in response to a signer key use limit information indicating that the signature key information is not already used, as recited in claim 23, and similarly recited for a computer program in claim 25.

For example, the specification discloses various exemplary aspects of a distribution information management system including a data carrier (1) attached to an article for storing its information, a distribution information processing module (2) that interfaces data carrier (1) for the article information, and a distribution information management module (3) that manages the information for distribution of the article, as shown in Fig. 1. The distribution information processing module (2) includes reading part (4) that reads out the information from the data carrier (1), a storing part (5) that stores the information, a first information verification unit (6) that verifies the information, an information generating unit (7) that processes the information, and a first communication part (8) that communicates (at step S503) with the distribution information management module (3). See the specification, for example, at pages 17-19 and Fig. 1.

In addition, first information verification unit (6) includes a first information verification part (9) that verifies the information using a verification key, and a first verification key storage part (10) that stores the verification key used by the first information verification part (9). The first verification unit (6) optionally includes a first verification key selection part (29) that selects the verification key used by the first information verification part (9). See for example, page 28 and Fig. 6.

The information generating unit (7) includes a distribution information generating part (11) that generates the information to be stored in the data carrier (1), a signature module (12) that performs signature generating process, a signature key information storage part (14) that stores the signature key information used by the signature module (12) for generating an digital signature, a signature key information selection part (13) that selects a signature key information stored in the signature key storage part (14), and a signature key information acquisition part (15) that acquires the signature key information from the distribution information management module (3). See, for example, page 24 and Figs. 3-4.

The signature module (12) includes a signature part (16) that generates a digital signature (at steps S415-416) for the information generated by the distribution information generating part (11), a first signer private information storage part (17) that stores signer private information (at step S1010) used by the signature part (16) for generating the digital signature, and a signature key use limit information storage part (27) that stores and updates (at step S1012) a signer key use limit information to indicate whether the signature key information has already been used (at step S1112), to prevent the signer from exceeding the authorization provided for the signature. See, for example, pages 33 and 37, and Figs. 9-11.

The distribution information management module (3) includes a second communication part (18) that communicates with the distribution information processing module (2), a second information verification unit (19) that processes the information received from the distribution information processing module (2), and a signature key information generating unit (20) that processes the signature key information to be sent to the distribution information processing module (2). See pages 26 and 40. The signature key information generating unit (20) includes a signature key information generating part (23) that generates a signature key information used by the distribution information processing module (2) for generating a distribution information in response to a signer key use limit information indicating that the signature key information is not already used.

Instead, Bauer discloses a system for monitoring the condition of goods during distribution. In particular, Bauer teaches a control and monitoring unit 1 mounted on a transport container 5. In addition to an identification unit 15, sensors 13 and actuators 14 are provided for the goods to indicate mechanical stress of the goods during freight transport (col. 4, lines 39-66 and Figs. 1, 3 and 5 of Bauer).

Further, Sudia discloses a multistep signing method and apparatus to affix a signature using a plurality of signing devices 11, 13, 15, 17, 19 connected over a LAN/WAN network 21. In particular, Sudia teaches a signing device 2 to assign an identification code with a public/private key pair 12a, 12b for encrypting and decrypting communications and a separate public/private key pair 14a, 14b for signature verification, together with public encryption and verification keys 16, 18 for other signing devices (paragraphs [0043] – [0044] and Fig. 1 of Sudia).

Neither Bauer nor Sudia teaches limiting a signer's ability to provide a verifiable signature by information for use limit of the signature key, nor is there any suggestion for such features, as provided in Applicants' claims 1, 18 and 20-27. These reasons apply by extension to claims 2-17 based on their dependence from claim 1, as well as to claim 19 based on its dependence from claim 18.

Further, there is would have been no motivation to combine features related to the condition monitoring of Bauer with the cryptographic roaming of Sudia, nor has the Office Action established sufficient motivation for a *prima facie* case of obviousness. The types of problems addressed by these respective references are entirely unrelated, in particular, goods environment monitoring for Bauer and network signature key distribution for Sudia. The disparity in subject matter of the references negates any motivation by one of ordinary skill to combine their teachings. Even assuming that motivation to combine the applied references is established, the combination fails to teach or suggest Applicants' claimed features.

A *prima facie* case of obviousness for a §103 rejection requires satisfaction of three basic criteria: there must be some suggestion or motivation either in the references or knowledge generally available to modify the references or combine reference teachings, a reasonable expectation of success, and the references must teach or suggest all the claim limitations (MPEP §706.02(j)). Applicants assert that the Office Action fails to satisfy these requirements with Bauer and Sudia.

For at least these reasons, Applicants respectfully assert that the independent claims are now patentable over the applied references. The dependent claims are likewise patentable over the applied references for at least the reasons discussed, as well as for the additional features they recite. Consequently, all the claims are in condition for allowance. Thus, Applicants respectfully request that the rejection under 35 U.S.C. §103 be withdrawn.

In view of the foregoing amendments and remarks, Applicants respectfully submit that this application is in condition for allowance. Favorable reconsideration and prompt allowance are earnestly solicited.

Should the Examiner believe that anything further is desirable in order to place this application in even better condition for allowance, the Examiner is invited to contact Applicants' undersigned representative at the telephone number listed below.

Respectfully submitted,

James A. Oliff
Registration No. 27,075

Gerhard W. Thielman
Registration No. 43,186

JAO:GWT/gwt

Attachment:
Replacement Drawing Sheets (Figs. 1-24)

Date: March 29, 2005

OLIFF & BERRIDGE, PLC
P.O. Box 19928
Alexandria, Virginia 22320
Telephone: (703) 836-6400

DEPOSIT ACCOUNT USE
AUTHORIZATION
Please grant any extension
necessary for entry;
Charge any fee due to our
Deposit Account No. 15-0461